GO COMMITTEE #1
September 18, 2014

MEMORANDUM

September 16, 2014

TO: Government Operations and Fiscal Policy Committee

FROM: Dr. Costis Toregas, Council IT Adviser CT

SUBJECT: Update – Cybersecurity

Expected to attend:

Sonny Segal, Chief Information Officer, Department of Technology Services
Keith Young, Enterprise Information Security Officer, Department of Technology Services
Michael Ferrara, Executive Director of Enterprise Projects, Office of the County Executive
Larry Dyckman, Manager, Office of Internal Audit

Staff recommendations:

1. The Committee should request a briefing in late November to assess the outcomes of the information security assessment studies being currently undertaken.
2. The Committee should encourage the Executive to consider new organizational responses to cybersecurity management by:
   a. centralizing cybersecurity functions across all departments; and
   b. addressing cybersecurity issues, not from within the narrow confines of a technology department, but from a broader perspective of Risk Management or Emergency Operations.
3. The Committee should encourage the Executive to improve the mix of actions vs. studies by rapidly implementing more low-cost or no-cost cybersecurity strategies while necessary studies are being carried out; examples of such actions are:
   a. Request current IT systems vendors and contractors to improve their own cybersecurity posture.
   b. Ensure that all IT personnel (both within DTS and in other departments with IT staff) expand their levels of certifications and training in cybersecurity skill sets.
   c. Encourage ITPCC to undertake cybersecurity operational improvements at the cross-agency level.
   d. Require cybersecurity expertise from all new hires and vendors going forward.

Background

The Committee has asked to be briefed on the status of the three ongoing efforts related to strengthening the cybersecurity posture of the County and, more specifically, to understand the differences in scope, project management, and expected outcomes of three major information security assessments. The County Executive has provided a report detailing the status on © 1-11, and representatives from the organizations responsible for the direction of these efforts will be available to provide additional clarity.

Discussion

The three information assessment projects are summarized in the table below:

PROJECT	PERFORMER	RESPONSIBLE	COMPLETION	COST
IT Security Assessment	Gartner Corporation	CAO's Office- Michael Ferrara	December 2014	Firm fixed price of $184,515 and a variable element not to exceed $45,090
High-level Risk Assessment of IT Systems	Watkins Meegan	Internal Audit- Larry Dyckman	November 2014	Firm fixed price of $53,040 for Phase I; Phase II not yet costed out
In-depth Risk Assessment and Penetration Testing	To be selected	Department of Technology Services- Keith Young	Not currently known	$100,000 available in FY15 DTS operating budget

The outcomes of the first two studies will be reports of assessments, and there is no expectation that any remedial action will be included. The second part of the third study (penetration testing) will in fact be the only place where an actual set of recommendations for strengthening a specific system will be made and carried out; the actual implementation of these recommendations may or may not find funding in the FY15 budget and may need additional appropriations through a supplemental process.

This preponderance of studies before major actions are undertaken is wise, since the sheer number and size of the systems currently under possible cyber attack make an immediate remediation of the risk in all systems an expensive proposition. In addition, Committee members must also remember that there are ongoing efforts within the current cybersecurity program that remediate threats and deter attacks on a daily basis. However, the seeming lack of action items arising from these studies in FY25 may have to be addressed by undertaking more visible efforts to assure residents and employees alike that progress is being made.

The one area of high importance is to ensure that these assessments not only concentrate on technology systems, but on people and the processes they undertake in order to move the County forward. The Executive states that, indeed, the assessments will focus on this continuum of levels – technology to system to process to human behavior – and therefore the Committee will have to await the final reports for evidence that this indeed occurred.

Council staff offers the following observations to provide a foundation for further discussions that can pave the way for both possible current operational improvements and a budgetary framework for FY16.

1. From Cybersecurity to Risk Management

   On March 14, 2014, GO Committee Chair Nancy Navarro wrote a letter on behalf of the GO Committee to the County CIO, stating that "...it is not a question of if Montgomery County government will be targeted, but when...". This statement is reflective of the reality recognized by cybersecurity experts and government policy experts alike. If one accepts the fact that an attack is not preventable and that a breach is inevitable, the optimal path is not one of solely securing systems but of managing the risk under the assumption that one or more systems may indeed be breached. This takes the analysis well beyond the realm of technology vulnerabilities, as a breached system presents financial exposure, liability and challenges of valuation and insuring against such risk. Business continuity costs, estimating risk of lawsuits or recovering data and re-starting destroyed processes may need non-technology skills to be properly assessed.

   Management of cyber risk requires additional skills beyond those of computer systems, and the County would be well-served to begin exploring new ways of managing and administering this evolving threat. Both the Risk Management office and the Office of Emergency Preparedness may have to be given a far greater role in future budgets in order to accommodate this new and evolving perspective.

2. Federated to Centralized Cybersecurity Administration

   Currently there are many departments within County government that manage their own IT assets, well beyond the Department of Technology Services. The County has a "federated" organizational structure under which major departments such as Police, Transportation, and Health & Human Services have their own independent technology organizations that are loosely "federated" within the DTS structure. In an early analysis in 2009, the Office of Management and Budget estimated that at least $18.1 million was invested for IT in organizations other than DTS, and this large number has probably grown since that time.

   These independent IT organizations in each major department may provide for flexible and more responsive ways to develop and manage IT assets for the department. However, in this era of interdependencies, one false step against a cyber intruder may jeopardize not just the independent department, but also the entire County enterprise. Private and governmental organizations have therefore begun to consider strategies to centralize the cybersecurity aspects of information systems under a unified leadership structure in order to better manage enterprise risk. The County should consider a similar strategy in the next budget cycle.

   When combined with the first observation regarding the placement of cybersecurity outside the IT organization, the combined change of centralization of the cybersecurity function under a new organizational structure may be a complex and harsh undertaking. However, the risk of inaction or "business as usual" is so high that bold and seemingly extraordinary strategies such as #1 and #2 may indeed be necessary.

3. Rapid, Low Cost, or No Cost Actions

The Executive has chosen a prudent path of assessment to safeguard resources and target them to systems that can be shown to be vulnerable and high priority. However, it is possible to also show progress over multiple fronts by undertaking simple actions against cyber attacks while the studies are underway but before they can produce the required results. Examples of such actionable strategies that could be done for little or no cost include:

i. All current and future IT services and systems vendors could be asked to document and improve (where warranted) their cyber-security protection.

ii. IT personnel within DTS and other departmental IT organizations may be lacking in cybersecurity skill sets and industry certifications, but it is hard to assess and improve without focusing attention on this. Working with OHR, a review of current certifications can be made and, where warranted, additional training or education provided to strengthen the cyber defense against attacks beyond the small number of cybersecurity professionals; in other words, the entire IT complement of all departments should be made part of the cybersecurity strategy and actions.

iii. The Interagency Technology Policy and Coordination Committee (ITPCC) work program has a cybersecurity element; this can be given additional priority and encouraged to explore cross-agency cybersecurity operational and tactical efforts with a short implementation time frame.

iv. The procurement solicitations for all technology products going forward should provide a beefed-up section on cybersecurity requirements to be met by the successful vendor. In addition, all new hires of personnel may give preference to those with proven cyber skills or industry certifications, whether in the IT function or elsewhere in the organization.

These are examples of strategies and are by no means exhaustive. They are intended to suggest immediate actions that can provide examples of visible leadership and practical strengthening of the County posture while the risk assessment studies take their course.

GO Committee Briefing
Information Security Assessments
Sept. 18, 2014

Summary

The County Executive and County Council are committed to reducing risk to the County's computer systems and infrastructure, sensitive data and business operations. At the CAO's request, the Department of Technology Services (DTS) developed a high-level FY14-FY17 Strategic Plan for Enterprise Security and Information Risk Management (SPES) and a recommended information/cyber security implementation acceleration plan in FY14. The CAO approved the acceleration of some of the activities on the plan and requested the following three independent, expert assessments:

I. IT Security Assessment
II. High-level Risk Assessment of IT Systems
III. In-depth Risk Assessment and Penetration Testing

These interdependent activities are described in detail below. Activity I is an independent review of the County's security program along with the items recommended for acceleration by DTS for FY15 and FY16. Activity II validates the County's systems inventory, leverages the previously completed data set inventory, and assigns risk ratings to systems in order to assist the County in determining the order in which systems should be subjected to further risk assessment and testing for vulnerability identification. Activity II will also provide estimated cost ranges for penetration testing and remediation of the highest value systems. Activity III is an in-depth risk assessment and penetration testing of one or more high value systems.

These activities are in addition to ongoing security program initiatives and are expected to enhance the program. All three activities are in alignment with the strategic objectives, principles and high level road map in the County's SPES. For reference, a summary table of initiatives from the SPES is provided at the end of this document.

The discussion below provides the following information about each of the above activities:

a. Context, Methodology and Importance
b. Responsibility for Managing the Project

c. Expected Outcomes
d. Expected Costs and Budget Lines
e. Alignment with the Specific Strategic Objectives in the County's SPES

Background
The County's SPES was briefed to the GO Committee on March 31, 2014. It contained the following strategic objectives:

1. *Continue to enhance the use of secure and stable cloud technologies*
2. *Secure County data on legacy and next generation devices*
3. *Manage users of all County services, systems, and applications*
4. *Assess requirements and recommend reasonable risk solutions*
5. *Modify enterprise user behavior to improve overall security/privacy posture*
6. *Streamline and automate security*

The County's information security program includes ongoing activities in support of the above objectives. DTS recommended the acceleration of the most urgent activities in FY14 and FY15. These recommendations were based on a number of considerations:

1. Further reduce risk to operations in an accelerated timeframe
2. Safeguard against a rapidly changing threat environment (as evidenced by notifications of breaches elsewhere)
3. Accelerate technology upgrades and move to more secure platforms
4. Achieve or maintain compliance with the law or industry requirements
5. Address audit findings

Prior to approving the acceleration of the remaining activities, the CAO has decided to undertake multiple independent risk assessments at various levels to inform decisions in the next three years relating to funding, policy, operations and technology.

I. IT Security Assessment

a. Context, Methodology and Importance

This is a strategic assessment by an independent expert of the County's information security program. It will include an assessment of the current program at the people, environment, processes, systems and infrastructure levels.

The importance of the project is to have independent experts conduct a review of the County's security program against best practices in order to inform investment decisions in FY15 and beyond.

The methodology will include a review of the County's existing information security program, systems, documentation and practices, interviews with stakeholders (both DTS and non-DTS system and business owners), research of technical issues and platforms, comparison with benchmark information and (best practice) reference architecture, gap analysis, and written report and briefings on the findings and recommendations. The intent is to create a comprehensive County-wide security assessment encompassing not only systems, but also people, processes and policies.

In addition, a Director of Gartner Corporation's Information Security Practice will serve as the expert advisor to the County's senior management on security planning and operational matters on an "on-demand" basis.

It should be noted that this assessment will use the output (or interim outputs) from the High-level Risk Assessment of IT systems (discussed below) as one of its inputs.

b. Responsibility for Managing the Project

The CAO retained the services of the Gartner Corporation in August 2014 to conduct this assessment. The project is being managed by the CAO's office.

c. Expected Outcomes

The project deliverables for the IT Security Assessment are expected in December 2014 and will include a security roadmap and architecture. The County will be able to use this information to validate the DTS recommended investments it must make, and the order it must make them in, to reduce security risk in an affordable and manageable manner over the next few years.

d. Expected Costs and Budget Lines

The IT Security Assessment task is awarded on a firm-fixed price of $184,515 and the Security Advisory Services task is awarded on a Time and Materials basis not to exceed the amount of $45,090. Both tasks are funded from the DTS FY15 Operating Budget.

e. Alignment with the Specific Strategic Objectives in the SPES

This IT Security Assessment supports all of the following strategic objectives in the County's SPES:

1. *Continue to enhance the use of secure and stable cloud technologies*
2. *Secure County data on legacy and next generation devices*
3. *Manage users of all County services, systems, and applications*
4. *Assess requirements and recommend reasonable risk solutions*
5. *Modify enterprise user behavior to improve overall security/privacy posture*
6. *Streamline and automate security*

II. High-level Risk Assessment of IT Systems

a. Context, Methodology and Importance

A high level risk assessment of the County's IT systems is necessary to identify the risk categories individual systems fall in so that they may be tested further for vulnerabilities in priority order. Initially, the three risk classification categories contemplated are high, medium and low risk.

This assessment should not be confused with the annual Health of IT Systems assessment provided to the GO Committee by the ITPCC members. The Health assessment is based on system age and operational factors.

At a high level, the methodology for this study includes:

- Validating the systems inventory
- Assigning system criticality according to the confidentiality, integrity and availability (CIA) model, along with type of sensitive data contained within the system and level of importance to the business unit
- Recommending a risk assessment strategy for the most critical systems

It should also be noted that fixing documented risks and retesting to assess residual risk are not in the scope of this project. Depending on the type and magnitude of the required remediation activities, they will be addressed by existing system maintenance and support programs and funding or may require additional future funding.

The above methodology will be applied in two phases as detailed below.

Phase 1
The objective of Phase 1 is to develop a baseline understanding of the County IT assets by first classifying them into different categories and then cumulating supplementary information to help focus the scope of the engagement based on criticality factors. Upon development of the baseline understanding of the County's IT assets and categorizing them, relevant criticality information will be collected from County departments and the systems will be ranked based on criticality. This will be followed by the creation of different tiers of assets (e.g., High, Medium, Low) based on criticality, and the systems will be classified in these tiers.

An IT Risk Assessment Plan will be developed in Phase 1 and if approved by the County it will be executed in Phase II on the agreed upon critical assets. The IT risk assessment will focus specifically on information security risk. Information security risk focuses on the risks associated with inappropriate access to systems, data or information. It encompasses areas of risk such as improper segregation of duties, risks associated with the integrity of data and databases, and information confidentiality. The consultants will work with the Office of Internal Audit and DTS to agree on the specific areas within information security risks that would be covered in the detailed IT Risk Assessment Plan.

Results of the above assessment will be reviewed by the Information Technology Policy Advisory Committee (IPAC) and in addition to being used to lower security risk, they will be used to inform continuity of operations plans (COOP) for the County's business critical systems in conjunction with the Office of Emergency Management and Homeland Security (OEMHS).

Phase 2
The objective will be to execute the IT Risk Assessment Plan (developed in Phase 1) specifically applying information security risk assessment criteria to the agreed upon critical assets. The result of Phase 2 will be to identify high-level information risks contained within the top critical assets which

manage highly sensitive and/or regulated information. It should be noted that the objectives of Phase 2 are not to assess the risk to all systems in the inventory, but instead only to agreed upon critical assets (i.e., a subset of the County's 600+ systems) based on criticality.

The importance of this project is to build a plan of system/data assessments in order to use available funding more wisely and to assess more critical systems earlier than later.

b. Responsibility for Managing the Project

The Office of Internal Audit retained the services of the Watkins Meegan Corporation in June 2014 to conduct this assessment. The project is being managed by the manager of the Office of Internal Audit.

c. Expected Outcomes

The project deliverables for Phase 1 of the High-level Risk Assessment of IT Systems are expected in November 2014 and will include a classification of the County's business applications classified by their highest risk. The County will be able to use this information to identify the investments it must make, and the order it must make them in, to reduce security risk in an affordable and manageable manner over the next few years.

d. Expected Costs and Budget Lines

Phase 1 of the High-level Risk Assessment of IT Systems is awarded on a firm-fixed price of $53,040. Phase 2 has not yet been priced. Phase 1 is funded from the Office of Internal Audit FY15 Operating Budget and Phase 2 will be funded by the DTS FY15 Operating Budget.

The following are the major differences between the IT Security Assessment by Gartner and the High-level Risk Assessment of IT Systems by Watkins Meegan:

1. The IT Security Assessment by Gartner will focus on conducting a high level assessment of the current security program/plan/posture of Montgomery County. More specifically it will concentrate efforts on governance, including policies, procedures, and standards. The High-level Risk Assessment of IT Systems by Watkins Meegan is focused on assigning criticality to individual IT systems so the County can successfully plan a system risk

assessment and penetration strategy. There will be a slight overlap between the two studies because the High-level Risk Assessment of IT Systems will also need to examine the suitability of enterprise policies, procedures, and standards regarding system security.

2. Gartner will meet with County officials at the senior, policy level. Watkins Meegan will be meeting with system and business owners as well as IT officials within the departments including DTS that operate the various IT systems.
3. The Gartner study will focus on advising the County on any improvements needed in its funding strategy to meet regulatory and mission needs. Therefore it may be stated that Gartner's efforts are primarily future oriented and will influence larger strategies with a longer-term focus on maturing the security program gradually and sustaining its strengths. The Watkins Meegan study, on the other hand will concentrate on helping the County prepare for a cost-effective audit and penetration testing strategy, while also commenting on any deficiencies in the present security architecture that need immediate corrective action.

e. Alignment with the Specific Strategic Objectives in the SPES

The High-level Risk Assessment of IT Systems initiative supports the following strategic objectives in the County's SPES:

1. *Continue to enhance the use of secure and stable cloud technologies*
2. *Secure County data on legacy and next generation devices*
3. *Assess requirements and recommend reasonable risk solutions*

III. In-depth Risk Assessment and Penetration Testing

a. Context, Methodology and Importance

As stated above, this project is to conduct the actual penetration testing and in-depth risk assessment for one or more system in the highest risk tier(s) according to the results of the High-level Risk Assessment of IT Systems conducted by Watkins Meegan.

The methodology will include providing the third-party auditor with general information about the systems to be tested. Unlike the previous activities, the in-depth risk assessment will examine detailed technical, operational, and managerial controls in the specific systems. The importance of penetration testing is to demonstrate potential "real-world" exploitation of known and unknown vulnerabilities in select County systems.

b. Responsibility for Managing the Project

Penetration testing will be awarded competitively using the County's IT Professional Services set of contracts. The DTS Enterprise Information Security Office will be responsible for managing the task orders. The results will be shared with the expert consultant from Gartner.

c. Expected Outcomes

The system focused risk assessment and penetration testing will result in a detailed vulnerability report and will include remediation actions required. Risk assessment and penetration testing experience will guide the County's efforts to prioritize and fund future system-specific security improvements.

d. Expected Costs and Budget Lines

Funding to conduct risk assessments and penetration testing of one of the County's highest risk systems was included in the DTS FY15 Operating Budget in the amount of $100,000.

e. Alignment with the Specific Strategic Objectives in the SPES

The In-depth Risk Assessment and Penetration Testing initiative supports the following strategic objectives in the County's SPES:

1. *Continue to enhance the use of secure and stable cloud technologies*
2. *Secure County data on legacy and next generation devices*
3. *Manage users of all County services, systems, and applications*
4. *Assess requirements and recommend reasonable risk solutions*
5. *Modify enterprise user behavior to improve overall security/privacy posture*
6. *Streamline and automate security*

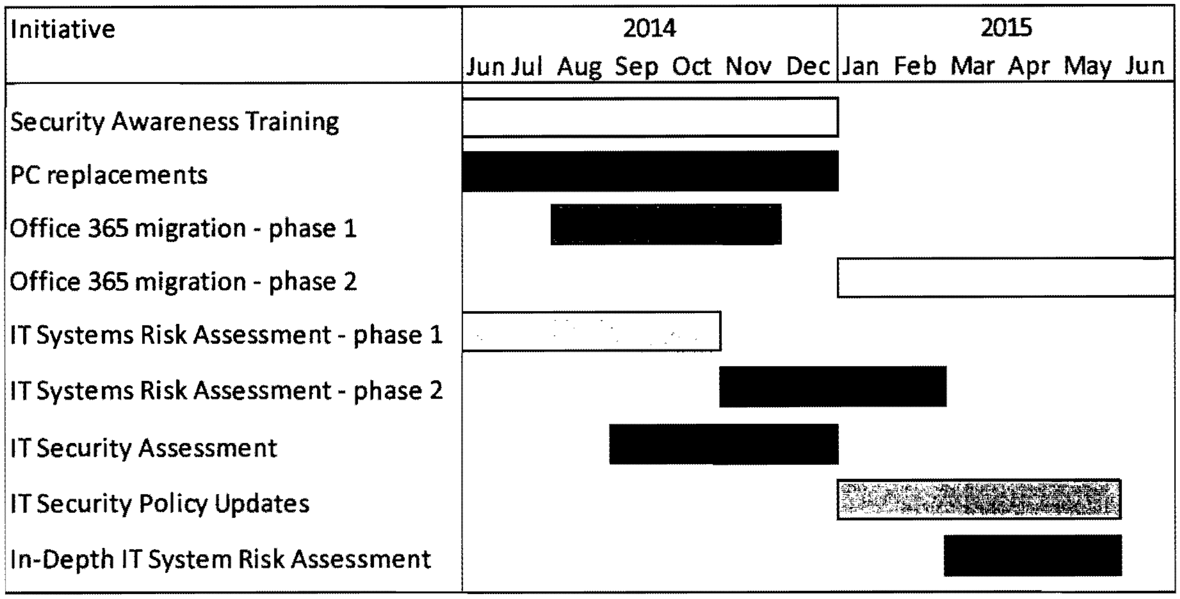
IV. Additional Benefits

a) The above assessments together provide the County an assessment of the "reasonable" controls and investment of resources and effort required to lower information security risk to its assets in the most cost-effective manner. In other words, these assessments will allow the County not only to prioritize its investments in information security but will also safeguard against over investment in areas of low returns or priority. This is important because the normal reaction to news of breaches elsewhere is to rapidly invest money and resources in all possible activities without realizing that the total cost of a "shotgun" security program is potentially unaffordable and possibly not as effective as one that is implemented in a planned manner commensurate with the risk tolerance demands of the organization, compliance requirements, and existing system, data assets and computing and communications architectures.

b) While the scope of the assessments discussed above is limited to the County government, the experience gained from the above assessments could be valuable to all the member agencies of the ITPCC. We will continue to update the ITPCC CIOs and CISOs on the findings as a part of the ITPCC Work plan.

V. Timeline

In addition to the three Information Security Assessment initiatives detailed in above, two additional IT security related initiatives are included the in the following timeline.



VI. SPES Roadmap Summary

The table below structures and prioritizes the roadmap items from the Strategic Plan for Enterprise Security and Information Risk Management. Specific timelines are not provided since funding depends on County Executive and Council priorities. As needed, this work plan and program priorities will be continually adapted to address emerging threats and new technologies.

	Short-Term	***Medium-Term***	***Long-Term***
Low Cost(<$50k)	- Increased focus on desktop vulnerability remediation - Cyber Maturity Assessment - Increased TOMG involvement	- Presentation to County-wide or targeted audience - BYOD Policy - Employee rules of behavior	- CyberSecurity Awareness Month event
Medium Cost ($50-150k)	- Expand awareness training - Expand security monitoring of critical infrastructure/ systems	- Cloud security framework and recommendations - Provide regular security awareness reminders and updates - Security Executive dashboard	- Enhanced user monitoring - Build 3rd-party assessment framework - Large project IT system assessments

		- Increased focus on application vulnerability remediation	
Higher Cost (> $150k)	- Enterprise Risk Assessment and Penetration Test	- Online Collaboration - Redact vs. retain policies - Mobile Device Management solution - Strengthen Identity Management Policies/ Procedures	- Strong Authentication - Ongoing regulatory compliance - Continued build-out and automation of incident response capabilities - Design and build COOP and Disaster Recovery into cloud migration